



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/041,964	01/09/2002	Makoto Oka	SON-2320	4260

7590 04/03/2006

RADER, FISHMAN & GRAUER, P.L.L.C.
Suite 501
1233 20th Street, NW
Washington, DC 20036

EXAMINER

POWERS, WILLIAM S

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 04/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/041,964	OKA ET AL.	
	Examiner	Art Unit	
	William S. Powers	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 January 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-36 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 January 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

In light of Applicant's amendments, all prior objections to the drawings are withdrawn.

In light of Applicant's amendments, all prior objections to the claims are withdrawn.

In light of Applicant's amendments, all previous 35 USC 101 rejections are withdrawn.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 13, 22 and 35 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 13, 22 and 35 are indefinite because they claim, "each of said plurality of signature modules respectively executes multiple signature algorithms", whereas the independent claims 1, 14 and 23 specify, "a plurality of signature modules each

executing a *different signature algorithm*." (Emphasis added) In the independent claims, each signature module executes a single, different signature algorithm. The dependent claims seek to broaden the base claim by claiming that each signature module executes multiple signature algorithms.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6. Claims 1-3, 5, 6, 8-12, 14-21, 23-25, 27, 28, 30-34 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 5,659,616 to Sudia in view of US Patent No. 6,035,402 to Vaeth et al. (hereto referred to as Vaeth) in further view of US Patent No. 6,490,680 to Scheidt et al. (hereinafter Scheidt).

As to claims 1, 14, 23 and 36, Sudia teaches a certificate authority for issuing a public key certificate used by an entity (column 5, lines 61-67). Sudia further teaches a plurality of signatures and attributes that are chosen by the certificate authority to create a secure certificate (Sudia, column 9, lines 13-46). Sudia does not expressly mention the use of a registration authority. However, in an analogous art, Vaeth teaches a registration authority which, on receiving a public key certificate issuance request from any one of entities under jurisdiction thereof, transmits the received request to said certificate authority (column 8, lines 35-48).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the certificate authority of Sudia with the registration authority of Vaeth in order to determine information required for identity verification as suggested by Vaeth (column 8, lines 3-6).

Neither Sudia nor Vaeth expressly state that the certificate authority uses a table with the signatures in the selection process. However, in an analogous art, Scheidt teaches said certificate authority (Credential Manager), having a plurality of signature modules each executing a different signature algorithm, selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority with reference to a table (database) that associates the registration authority with an assigned signature algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate (the Constructive Key Management System manages the encryption algorithms that are used to by an entity including selecting the appropriate digital signature(s) to apply to a certificate from a database that stores algorithms associated with users and policy restrictions/attributes) (column 7, line 44-column 8, line 62).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the certification and registration authorities that issue multiple signature certificates of Sudia and Vaeth with the database of Scheidt in order to "allow flexible access for authorized users of a communication system authorized while maintaining security for data at rest and in transit on the system," as suggested by Scheidt (column 1, lines 44-47).

As to claims 2, 15 and 24, Sudia, as modified, teaches:

- a. Said certificate authority has a certificate authority server for outputting a signature processing request to said plurality of signature modules (Constructive Key Management System) (Scheidt, column 7, lines 29-43).
- b. Wherein said certificate authority server receives said public key certificate issuance request from said registration authority, selects at least one of said plurality of signature modules in response to said public key certificate issuance request, and outputs said signature processing request to the selected signature module (Constructive Key Management System manages the creation and distribution of certificates and applies the appropriate signature(s) to the certificates to satisfy the policies dictated by the type, destination and purpose of the certificate) (Scheidt, column 7, line 44-column 8, line 62).
- c. Wherein each of said plurality of signature modules attaches a digital signature to the message data constituting said public key certificate in response to said signature processing request received from said certificate authority server (Scheidt, column 8, lines 46-62).

As to claims 3 and 25, Sudia, as modified, teaches:

- a. Wherein said certificate authority has a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with a signature algorithm specific to each of said registration authorities (database

maintained by the Credential Manager that keeps track of the credentials of a user) (Scheidt, column 8, lines 1-62).

b. Wherein, given a public key certificate issuance request from any registration authority, said certificate authority selects the signature module associated with the relevant signature algorithm based on said registration authority management data (Scheidt, column 8, lines 46-62).

As to claims 5 and 27, Sudia, as modified, teaches that said registration authority management data include signature module identification information applicable to signatures (database with signature algorithms associated with respective users) (column 8, lines 10-17 and lines 46-62).

As to claims 6 and 28, Sudia, as modified, teaches said registration authority transmits signature algorithm designation information along with said public key certificate issuance request to said certificate authority; and wherein said certificate authority, based on said signature algorithm designation information received along with said public key certificate issuance request, selects a signature module applicable to the designated signature algorithm (selecting signature algorithm according to user and certificate needs) (column 8, lines 46-62).

As to claims 8 and 30, Sudia, as modified, teaches:

- a. Said certificate authority has a verification key database which stores keys for signature verification in association with each of said plurality of signature modules (authorization certificates) (Sudia, column 7, lines 37-67).
- b. Wherein said certificate authority verifies signatures generated by each of said plurality of signature modules (Sudia, column 12, lines 19-44).

As to claims 9, 19 and 31, Sudia, as modified, teaches said certificate authority uses at least two of said plurality of signature modules to attach at least two different digital signatures to one public key certificate (the use of co-signatories for a certificate that requires authorization over that of the original signatory) (Sudia, column 9, lines 38-46).

As to claims 10, 20 and 32, Sudia, as modified, teaches wherein said certificate authority selects at least two of said plurality of signature modules in order to have signature processing executed in steps by each of the selected signature modules used in concert for digital signature generation (the use of co-signatories for a certificate that requires authorization over that of the original signatory) (Sudia, column 9, lines 38-46).

As to claims 11 and 21, Sudia, as modified, teaches:

- a. Said certificate authority and said registration authority each have a signature module structure management table which associates signature algorithm identifiers with identifiers of said plurality of signature modules (the

Constructive Key Management System manages the encryption algorithms that are used to by an entity including selecting the appropriate digital signature(s) to apply to a certificate from a database that stores algorithms associated with users and policy restrictions/attributes) (Scheidt, column 7, line 44-column 8, line 62).

b. Wherein said registration authority issues to said certificate authority a public key certificate issuance request designating a signature algorithm identifier in accordance with said signature module structure management table (the Constructive Key Management System manages the encryption algorithms that are used to by an entity including selecting the appropriate digital signature(s) to apply to a certificate from a database that stores algorithms associated with users and policy restrictions/attributes) (column 7, line 44-column 8, line 62).

c. Wherein said certificate authority, upon receipt of said signature algorithm identifier from said registration authority, selects the signature module applicable to the received identifier from said signature module structure management table (Constructive Key Management System manages the creation and distribution of certificates and applies the appropriate signature(s) to the certificates to satisfy the policies dictated by the type, destination and purpose of the certificate) (Scheidt, column 7, line 44-column 8, line 62).

As to claims 12 and 34, Sudia, as modified, teaches at least part of said plurality of signature modules have a common signature key stored therein (the certificate is

signed by the certificate authority's private key, thereby having that key in common with all the signatures appended to the certificate) (Sudia, column 17, lines 21-25).

As to claim 16, Sudia, as modified, teaches said certificate authority server selecting the signature module comprises selecting the signature module based on a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with a signature algorithm specific to each of said registration authorities (database maintained by the Credential Manager that keeps track of the credentials of a user) (Scheidt, column 8, lines 1-62).

As to claim 17, Sudia, as modified, teaches said certificate authority server selecting the signature module comprises selecting the signature module based on signature algorithm designation information received along with said public key certificate issuance request (Scheidt, column 8, lines 46-62).

As to claim 18, Sudia, as modified, teaches causing said certificate authority to verify signatures generated by each of said plurality of signature modules (Sudia, column 12, lines 19-44).

As to claim 33, Sudia, as modified, teaches:

- a. A signature module structure management table which associates signature algorithm identifiers with identifiers of said plurality of signature modules; (the Constructive Key Management System manages the encryption algorithms that are used to by an entity including selecting the appropriate digital signature(s) to apply to a certificate from a database that stores algorithms associated with users and policy restrictions/attributes) (Scheidt, column 7, line 44-column 8, line 62).
- b. Wherein said digital certification apparatus, upon receipt of a signature algorithm identifier along with said public key certificate issuance request, selects the signature module applicable to the received identifier from said signature module structure management table. (Constructive Key Management System manages the creation and distribution of certificates and applies the appropriate signature(s) to the certificates to satisfy the policies dictated by the type, destination and purpose of the certificate) (Scheidt, column 7, line 44-column 8, line 62).

7. Claims 4, 7, 26 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 5,659,616 to Sudia in view of US Patent No. 6,035,402 to Vaeth et al. (hereto referred to as Vaeth) in further view of US Patent No. 6,490,680 to Scheidt et al. (hereinafter Scheidt) as applied to claims 1 and 3, claims 1 and 6, claims 23 and 25 and claims 23 and 28 respectively above, and further in view of US Patent No. 6,202,157 to Brownlie et al. (hereinafter Brownlie).

As to claims 4, 7, 26 and 29, Sudia, as modified, does not expressly mention storing the key length and parameter data of the signatures in the database. However, in an analogous art, Brownlie teaches management data that includes key length and parameter information applicable to signatures (column 3, lines 25-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the certification and registration authorities that select signature algorithms according to requirements of the certificate of Sudia, Vaeth and Scheidt with the storing of parameter information of the signature algorithms, including key length, of Brownlie in order to "allow enforcement of the policies to occur at the network nodes to help reduce overhead requirements of a central authority," as suggested by Brownlie (column 2, lines 31-33).

8. Claims 13, 22 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 5,659,616 to Sudia in view of US Patent No. 6,035,402 to Vaeth et al. (hereto referred to as Vaeth) in further view of US Patent No. 6,490,680 to Scheidt et al. (hereinafter Scheidt) as applied to claim 1, claim 14 and claim 23, respectively above, and further in view of US Patent No. 6,675,296 to Boeyen et al. (hereinafter Boeyen).

As to claims 13, 22 and 35, Sudia, as modified, does not expressly mention that the plurality of signature modules execute multiple signature algorithms. However, in an

analogous art, Boeyen teaches each of said plurality of signature modules respectively executes multiple signature algorithms (a certificate generator that determines the type of signature needed for a certificate and a signature selector that then selects the appropriate private key to use for the signing operation) (Boeyen, column 6, line 62-column 7, line 18).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the certification and registration authorities that select signature algorithms according to requirements of the certificate of Sudia, Vaeth and Scheidt with the multiple signature algorithm modules of Boeyen in order to "allow users of differing security infrastructures to communicate information using their respective certificates even though the certificates are in different formats" as suggested by Boeyen (column 7, lines 26-30).

Response to Arguments

9. Applicant's arguments filed 1/05/2006 have been fully considered but they are not persuasive.

10. In response to applicant's arguments that "Sudia has no disclosure of any kind regarding a registration authority", "it is unclear how Vaeth can in any way be construed as disclosing or suggesting selection by a certifying authority of a particular signature module" and "there is no apparent disclosure or suggestion in Brownlie of a certifying authority that has a plurality of signature modules", one cannot show nonobviousness

by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

11. In response to applicant's argument that there is no suggestion to combine the references of Sudia and Vaeth, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, both references are classified in class 380, subclass 23. Additionally, both patents deal with certificate authorities assigning signatures to certificates in a secure manner and ensuring all restrictive attributes required by the end-user are satisfied.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not


Art Unit: 2134

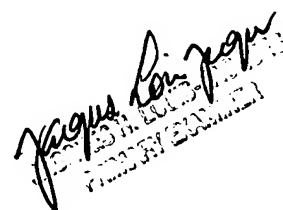
mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to William S. Powers whose telephone number is 751 272 8573. The examiner can normally be reached on m-f 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on 571 272 6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


William S. Powers
Examiner
Art Unit 2134


Jacques Louis-Jacques
Supervisor
Art Unit 2134